UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/804,852 | 03/19/2004 | Lauri Paatero | 915-008.022 | 7439 |

4955 7590 09/22/2010

WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

| EXAMINER | |
|---|---|
| TABOR, AMARE F | |
| ART UNIT | PAPER NUMBER |
| 2434 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 09/22/2010 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/804,852 | PAATERO, LAURI | |
| | Examiner | Art Unit | |
| | AMARE TABOR | 2434 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *01 July 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1,4 and 6-12* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,4 and 6-12* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. In view of the **PRE-APPEAL BRIEF** filed on July 01, 2010, **prosecution is hereby reopened**.

2. A new ground of rejection is set forth below.

3. To avoid abandonment of the application, appellant must exercise one of the following two options: (1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or, (2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

4. A Supervisory Patent Examiner (SPE) has approved of reopening prosecution by signing below:

5. /Kambiz Zand/

6. Supervisory Patent Examiner, Art Unit 2434

7. **Claims 1, 4 and 6-12** are pending.

### *35 USC § 103*

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

**Claims 1, 4 and 6-12** are rejected under 35 U.S.C. 103(a) as being unpatentable over Grohoski et al. (US 2004/0225885 A1, hereafter "**Grohoski**") in view of Moller et al. (US 2003/0014653 A1, hereafter "**Moller**")

As per Claim 1, Grohoski teaches:

An electronic device, comprising: an accelerator configured to accelerate cryptographic data processing operations [see Fig.2; and for example, par.0056], which accelerator comprises: a first logical interface over which data to be processed is provided [see 'transferring/receiving crypto-packet' in FIG.3; and for example, par.0061-0062], and a secure second logical interface over which cryptographic keys employed in processing data is provided [see 'control queue'/'securely sharing register/memory access' etc in FIGS.2-3 & 8; and for example, par.0052, 0056-0057, 0062 and 0106], wherein the first logical interface and the secure second logical interface share a same physical interface [see 'sharing same memory' in FIG.2; and for example, par.0056].

**Grohoski** teaches "a processor arranged in an electronic device" [see 'CRYPTO/CPU' arranged in microprocessor 200 in FIG.2]; but does not explicitly disclose "a configuration register configured to indicate to the accelerator whether secure mode or normal mode is set by a processor, and configured to receive mode setting instructions from a protected application" [see abstract and FIGS.1 and 3; 'protection control register (PCR)' enables/disables data interface in memory of processor] and "wherein the first logical interface is not accessible when data is transferred in the second logical interface" [see abstract and FIGS.2 and 4; and for example, par.0006-0014: when one interface is enabled, the other is disabled]. Therefore, it would have been obvious to a person having ordinary skill in the art at the time of applicant's invention was made to modify the system of **Grohoski** by incorporating protection control register (PCR) of **Moller**. An artisan would be motivated to modify in order to protect sensitive information stored in microprocessors [see at least par.0001 of **Moller**].

As per Claims 11 and 12, Grohoski-Moller combination teaches:

A device for acceleration of data processing operations, which device comprises: a first logical interface over which data to be processed is provided [see 'transferring/receiving crypto-packet' in FIG.3; and for example, par.0061-0062 of **Grohoski**]; and a secure second logical interface over which cryptographic keys employed in processing said data is provided [see 'control queue'/'securely sharing register/memory access' etc in FIGS.2-3 & 8; and for example, par.0052, 0056-0057, 0062 and 0106 of

**Grohoski**], wherein the first logical interface and the secure second logical interface share a same physical interface [see 'sharing same memory' in FIG.2; and for example, par.0056 of **Grohoski**], and a configuration registered configured to indicate to the device whether secure mode or normal mode is set by a processor, and configured to receive mode setting instructions from a protected application [see abstract and FIGS.1 and 3 of **Moller**; 'protection control register (PCR)' enables/disables data interface in memory of processor], said processor being arranged in the device [see 'CRYPTO/CPU' arranged in microprocessor 200 in FIG.2 of **Grohoski**], wherein the first logical interface is not accessible when data is being transferred in the second logical interface [see abstract and FIGS.2 and 4; and for example, par.0006-0014 of **Moller**: when one interface is enabled, the other is disabled].

As per Claim 4, Grohoski-Moller combination teaches:

The device according to claim 1, wherein the configuration register further is configured such that it may be set in one of a plurality of possible encryption modes, and the accelerator is configured to operate in the encryption mode set in the register [see 'encryption type field' in par.0116 of **Grohoski**].

As per Claim 6, Grohoski-Moller combination teaches:

The device according to claim 1, wherein the first logical interface of the accelerator is configured such that it is accessible by any application, while the secure second logical interface of the accelerator is configured such that it is accessible by protected applications only [see abstract and 'Set Protected Bit' in FIG.3 of **Moller**].

As per Claim 7, Grohoski-Moller combination teaches:

The device according to claim 6, wherein the protected applications are configured to prevent other applications from accessing the accelerator [see par.0106 of **Grohoski**].

As per Claim 8, Grohoski-Moller combination teaches:

The device according to claim 6, wherein the protected applications are applications which are allowed to execute in the secure execution environment [see abstract and FIGS.3-4 of **Moller**].

As per Claim 9, Grohoski-Moller combination teaches:

The device according to claim 1, further comprising: storage circuitry comprising at least one storage area in which protected data relating to device security are located [see par.0106 of **Grohoski**], and wherein the processor is configured to be set in one of at least two different operating modes [see of abstract and FIGS.1-2 **Moller**]; wherein the processor is given access to said storage area, in which said protected data are located, when a secure processor operating mode is set [see at least FIGS.2-4 of **Moller**], wherein the processor is denied access to said storage area when a normal processor operating mode is set [see 'Stop-Action'/'Erase Block 0' in FIG.4 of **Moller**]; and wherein the processor is capable of accessing the secure second logical interface of the accelerator, when the secure processor operating mode is set [see 'Enable'/'Set Protected Bit' in FIGS.2-3 **Moller**].

As per Claim 10, Grohoski-Moller combination teaches:

The device according to claim 9, wherein the processor is configured such that protected applications control the processor operation mode [see abstract and FIGS.2-3 of **Moller**].

## Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **AMARE TABOR** whose telephone number is (571)270-3155. The examiner can normally be reached on Mon-Fri 8:00a.m. to 5:00p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **KAMBIZ ZAND** can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Amare Tabor/
Examiner, Art Unit 2434

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2434